ABSTRACT OF THE DISCLOSURE

An optimization processing unit optimizes an input and output bit number of an S-box based on parameters inputted from an input unit. The examples of the parameters are memory capacity of a primary cache memory, entire input and output bit number, and smallest input and output number of the S-box. An S-box generating unit generates an S-box in accordance with the optimized input and output bit number of the S-box. Then, an F-function generating unit generates an F-function by aligning a plurality of S-boxes thus generated.